

ELECTRONIC DATA STORAGE SYSTEM, HISTORY VERIFYING DEVICE, ELECTRONIC DATA STORING METHOD AND RECORDING MEDIUM

Publication number: JP2001337600 (A)

Publication date: 2001-12-07

Inventor(s): NISHIZAWA HIDEKAZU

Applicant(s): TOKYO SHIBAURA ELECTRIC CO

Classification:

- international: G06F12/14; G06F12/00; G06F17/30; G06F21/24; G06K19/10; G09C1/00; G06F12/14; G06F12/00; G06F17/30; G06F21/00; G06K19/10; G09C1/00; (IPC1-7): G09C1/00; G06F12/00; G06F12/14; G06F17/30; G06K19/10

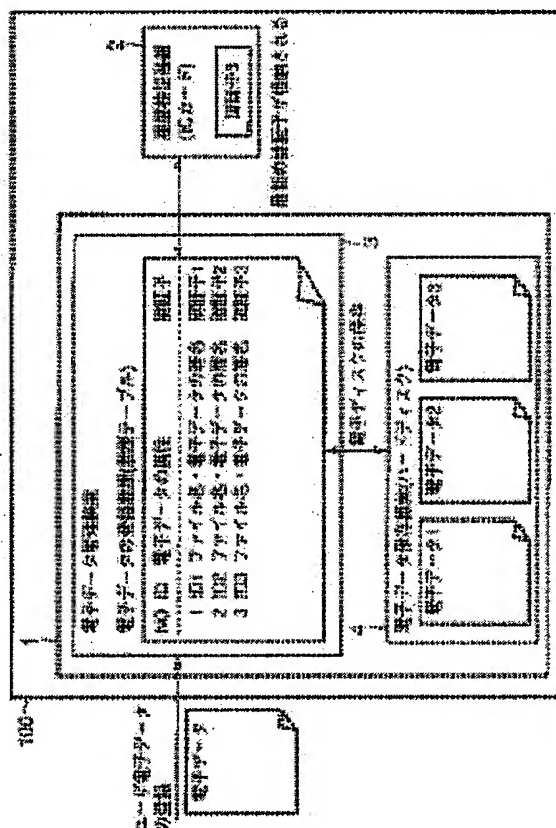
- European:

Application number: JP20000158728 20000529

Priority number(s): JP20000158728 20000529

Abstract of JP 2001337600 (A)

PROBLEM TO BE SOLVED: To provide an electronic data storage system, a history verifying device, an electronic data storing method and a recording medium by which electronic data can be prevented from being fraudulently altered or erased and detecting erasure and alteration of electronic data and capable of securing the original record performance of the electronic data can be secured.; **SOLUTION:** In this system 100 which has a history management device 5 for managing the history of stored electronic data and a history verifying device 2 which has a means for detecting the alteration of the history and a means for verifying that the history is the newest history and stores and manages the electronic data, the history management device 5 has a means for confirming that individual histories are not fraudulently altered, a means which prepares an identifier for verifying that the time sequential relation of histories is not fraudulently altered and verifies the relation. The history verifying device 2 stores the identifier of the newest history in the inside and a means 18 for verifying whether or not the verifier of the inside is matched with the identifier of the newest history of the history table.



Data supplied from the esp@cenet database — Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-337600
(P2001-337600A)

(43) 公開日 平成13年12月7日 (2001.12.7)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B 5 B 0 1 7 6 4 0 D 5 B 0 3 3
G 0 6 F 12/00	5 3 7	G 0 6 F 12/00	5 3 7 Z 5 B 0 7 5
12/14	3 1 0	12/14	3 1 0 Z 5 B 0 8 2
17/30	1 2 0	17/30	1 2 0 A 5 J 1 0 4
審査請求 未請求 請求項の数 8 O L (全 14 頁) 最終頁に続く			

(21) 出願番号 特願2000-158728(P2000-158728)

(22) 出願日 平成12年5月29日(2000.5.29)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 西澤 秀和

東京都府中市東芝町1番地 株式会社東芝
府中工場内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

Fターム(参考) 5B017 AA07 CA16

5B035 AA15 BB09

5B075 KK54 KK66

5B082 AA01 FA11 GA11

5J104 AA08 LA03 LA05 NA35 NA38

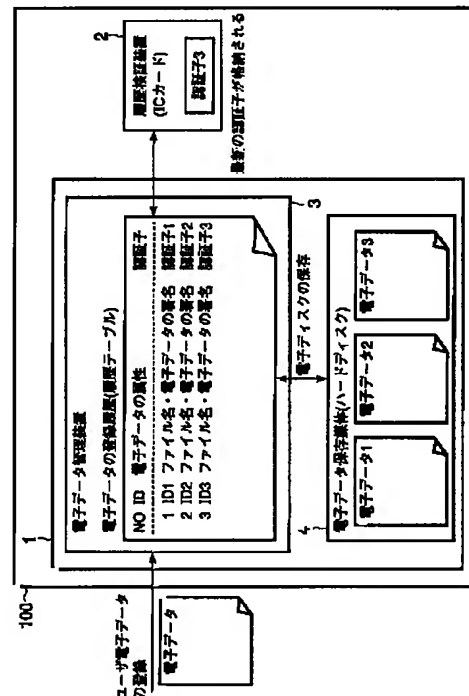
PA14

(54) 【発明の名称】 電子データ保管システム、履歴検証装置、電子データ保管方法及び記録媒体

(57) 【要約】

【課題】電子データの改ざん、消去の防止及び検知を可能にするとともに、電子データの原本性を確保することのできる電子データ保管システム、履歴検証装置、電子データ保管方法及び記憶媒体を提供すること。

【解決手段】電子データ保管の履歴を管理する履歴管理装置5と、履歴に対する改ざんを検知する手段および前記履歴が最新の履歴であることを検証する手段とを有した履歴検証装置2とを有した電子的なデータを保管し管理するシステム100において、履歴管理装置5は個々の履歴が改ざんされていないことを確認する手段と、履歴の時系列の関係が改ざんされていないことを検証するための認証子を作成し検証するための手段を有する。また履歴検証装置2は、最新の履歴の認証子を内部に保管し、内部の認証子と、履歴テーブルの最新の履歴の認証子が一致するか否かを検証する手段18を有する。



【特許請求の範囲】

【請求項1】 電子的なデータを保管し管理する電子データ保管システムにおいて、
電子データ保管の履歴を記憶する履歴テーブルを管理する履歴管理装置と、履歴検証装置とから構成され、
前記履歴管理装置は、
個々の履歴が改ざんされていないことを確認する確認手段と、
履歴の時系列の関係が改ざんされていないことを検証するための認証子を作成し検証するための検証手段と、を具備し、
前記履歴検証装置は、
個々の履歴に対する改ざんを検知する改ざん検知手段と、
最新の履歴の認証子を内部に保管し、前記内部に保管された認証子と前記履歴テーブルの最新の履歴の認証子の一致を検出することにより前記履歴が最新の履歴であることを検証する認証子検証手段と、を具備することを特徴とする電子データ保管システム。

【請求項2】 前記履歴検証装置は、前記最新の履歴の認証子を格納する最新認証子格納庫と、
履歴の更新と認証子を作成する認証子更新手段と、を備え、
前記最新認証子格納庫は外部からのアクセスが不可能であるように構成され、前記認証子更新手段により正当な手順を経て履歴が更新された場合にのみ前記最新認証子格納庫に格納された最新の認証子を更新することを特徴とする請求項1記載の電子データ保管システム。

【請求項3】 前記履歴検証装置は、前記履歴テーブルの履歴が改ざんされていないことを検証するための認証子検証手段を備え、
前記認証子検証手段は、前記履歴テーブルの最新の履歴の認証子と前記最新認証子格納庫の認証子が一致するか検証することを特徴とする請求項1記載の電子データ保管システム。

【請求項4】 電子的なデータを保管し管理する電子データ保管システムにおいて、
電子データ保管の履歴を記憶する履歴テーブルを管理する履歴管理装置と、最新の履歴の認証子を内部に保管する履歴検証装置と、から構成され、前記履歴管理装置は、個々の履歴が改ざんされていないことを確認する確認手段と、
個々の履歴の時系列の関係が改ざんされていないことを検証するための認証子を作成し検証するための検証手段と、
個々の履歴に対する改ざんを検知する改ざん検知手段と、
前記履歴検証装置から、最新の履歴の認証子を読み出し前記履歴テーブルの最新の履歴の認証子との一致を検出することにより前記履歴が最新の履歴であることを検証

する認証子検証手段と、を具備することを特徴とする電子データ保管システム。

【請求項5】 電子データの保管に際し、
電子データ保管の履歴の時系列の関係が改ざんされていないことを検証するための認証子の作成と、電子データが改ざんされていないことを検証するためのメッセージ認証子の作成とを行うための履歴検証装置にアクセスし、履歴の認証子及び電子データのメッセージ認証子を受け取る手順と、
履歴が改ざんされてなく、また最新の履歴であることを検証するために、前記履歴検証装置にアクセスし、検証結果を受け取る手順と、
を実行させるためのプログラムを記録したコンピュータ読取り可能な記録媒体。

【請求項6】 電子データ保管の履歴を記憶する履歴テーブルにおける個々の履歴が改ざんされていないことを確認する手順と、
履歴の時系列の関係が改ざんされていないことを検証するための認証子を作成する手順と、
最新の履歴の認証子を内部に保管する履歴検証装置から最新の履歴の認証子を読み出し、前記履歴テーブルの最新の履歴の認証子との一致を検証することにより前記履歴が最新の履歴であることを検証する手順と、を実行させるためのプログラムを記録したコンピュータ読取り可能な記録媒体。

【請求項7】 電子データ保管の履歴を管理する履歴管理装置と、履歴に対する改ざんを検知する手段と、前記履歴が最新の履歴であることを検証する手段を備えた履歴検証装置とから構成される、電子的なデータを保管し管理するシステムにおける電子データ保管方法において、

前記履歴管理装置は、履歴番号、識別子、属性情報、メッセージダイジェスト、及び前記履歴番号、識別子、属性情報、メッセージダイジェストのメッセージダイジェストを暗号化して得られる認証子から成る履歴情報を前記履歴検証装置に送信し、
前記履歴検証装置は、
前記履歴管理装置から送信された履歴番号、識別子、属性情報、メッセージダイジェスト及び認証子を受信し、これらの情報からメッセージダイジェストを作成し、
前記作成したメッセージダイジェストと1つ前の認証子との排他的論理和をとり、
前記履歴管理装置から送信された認証子を復号化し、前記排他的論理和により得られる値と比較し、
前記比較の結果、一致が得られたとき、前記履歴管理装置から送信された履歴情報が最新の履歴情報か否か判断し、
前記最新の履歴情報であるとき、前記履歴管理装置から送信された認証子と前記履歴検証装置内の最新認証子格納庫に保管されている最新認証子とを比較し、その比較

結果を前記履歴管理装置に送信する、ことを特徴とする電子データ保管方法。

【請求項 8】 電子的データ保管の履歴を管理する履歴管理装置と、履歴が最新の履歴であることを検証するための最新認証子を最新認証子格納庫に保管する履歴検証装置とから構成される、電子的なデータを保管し管理するシステムにおける電子データ保管方法において、前記履歴管理装置は、履歴番号、識別子、属性情報、メッセージダイジェスト、及び前記履歴番号、識別子、属性情報、メッセージダイジェストのメッセージダイジェストを暗号化して得られる認証子からなる履歴情報にもとづいてメッセージダイジェストを作成し、前記作成したメッセージダイジェストと 1 つ前の認証子との排他的論理和をとり、前記暗号化された認証子を復号化し、前記排他的論理和により得られる値と比較し、前記比較の結果、一致が得られたとき、前記履歴情報が最新の履歴情報か否か判断し、前記最新の履歴情報であるとき、前記履歴検証装置内の最新認証子格納庫から最新認証子を読み出し、前記履歴情報の認証子と比較し、履歴の時系列の関係が改ざんされているか否かを検証する、ことを特徴とする電子データ保管方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は電子データの改ざん、消去の防止および検知を可能とするとともに、電子データの原本性を確保する電子データ保管システム、履歴検証装置、電子データ保管方法および記憶媒体に関する。

【0002】

【従来の技術】新しい通信技術が導入されるとともにインターネットが爆発的に普及するにつれ、情報のセキュリティをいかに確保するかが重要な課題となっている。例えば、WWW(World Wide Web)サーバとブラウザ間でのセキュリティは、第三者によるデータの盗聴、改ざんの防止や第三者のなりすましによる被害を防止し、安全にデータのやり取りが行える環境を提供することにある。このためには、ネットワーク上を流れるデータを保護するために次の三つの機能を実現する必要がある。

【0003】すなわち、(1)ブラウザが通信している相手が本当のサーバであること(第三者によるなりすましのサーバでないこと)を保証するためのサーバ確認(Authentication)、(2)第三者によるデータの盗聴を防止するために転送するデータの暗号化(Encryption)、および(3)データの転送中にデータが改ざんされずに相手に送られたことを保証するデータ一貫性の保証(Data Integrity)の機能である。

【0004】サーバ認証は、電子証明書と公開鍵暗号

方式を用いて実現される。電子証明書は、サーバの名前(ドメイン名)やサーバの公開鍵、電子証明書の有効期間、電子証明書の認証機関の情報等のサーバの身分を証明する情報とそれらの情報が正しいことを保証する電子署名から構成される(図20参照)。電子署名はサーバの情報を基に作成され、認証機関の秘密鍵で暗号化される(図21参照)。サーバはこの電子証明書をブラウザ側に送ることにより、ブラウザが電子署名を復号して得られた情報と、証明書の内容を比較し、内容が一致すれば本当に正しいサーバと通信していることが証明される。

【0005】この仕組みは電子証明書に書かれている内容が正しい情報であることが前提となっている。このため、CA(Certificate Authorities)と呼ばれる認証機関が、証明書の請求に応じて、電子証明書を発行するように構成される。

【0006】

【発明が解決しようとする課題】上述したように、電子データ改ざん検知のために電子署名が用いられるが、従来は電子データ保管の履歴が改ざんされているか否かを検出する手段が無かったために、電子署名の付けられたデータについて、それが最新の改訂版なのか、すでに破棄されている過去の版のコピーなのか区別がつかず、電子データの原本性の保証ができないという問題があった。

【0007】本発明は上記事情に鑑みてなされたもので、その目的は、電子データの改ざん、消去の防止及び検知を可能にするとともに、電子データの原本性を確保することのできる電子データ保管システム、履歴検証装置、電子データ保管方法及び記録媒体を提供することである。

【0008】

【課題を解決するための手段】(1)本発明の電子データ保管システム(請求項1)は、電子データ保管の履歴を記憶する履歴テーブルを管理する履歴管理装置であって、個々の履歴が改ざんされていないことを確認する確認手段と、履歴の時系列の関係が改ざんされていないことを検証するための認証子を作成し検証するための検証手段と、を備えた履歴管理装置と、履歴に対する改ざんを検知する改ざん検知手段と、最新の履歴の認証子を内部に保管し、前記内部に保管された認証子と前記履歴テーブルの最新の履歴の認証子の一致を検出することにより前記履歴が最新の履歴であることを検証する認証子検証手段と、を備えた履歴検証装置、とを具備することを特徴とする。

【0009】本発明によれば、電子データの改ざん、消去の防止および検知が可能となるとともに、電子データの原本性が確保される。

【0010】(2)好ましくは(請求項2)、前記履歴検証装置は、前記最新の履歴の認証子を格納する最新認

証子格納庫と、履歴の更新と認証子を作成する認証子更新手段と、を備え、前記最新認証子格納庫は外部からのアクセスが不可能であるように構成され、前記認証子更新手段により正当な手順を経て履歴が更新された場合にのみ前記最新認証子格納庫に格納された最新の認証子を更新することを特徴とする。

【0011】(3) 好ましくは(請求項3)、前記履歴検証装置は、前記履歴テーブルの履歴が改ざんされていないことを検証するための認証子検証手段を備え、前記認証子検証手段は、前記履歴テーブルの最新の履歴の認証子と前記最新認証子格納庫の認証子が一致するか検証することを特徴とする。

【0012】(4) 本発明の電子データ保管システム(請求項4)は、電子的なデータを保管し管理する電子データ保管システムにおいて、最新の履歴の認証子を内部に保管する履歴検証装置と、電子データ保管の履歴を記憶する履歴テーブルを管理する履歴管理装置であって、個々の履歴が改ざんされていないことを確認する確認手段と、履歴の時系列の関係が改ざんされていないことを検証するための認証子を作成し検証するための検証手段と、履歴に対する改ざんを検知する改ざん検知手段と、前記履歴検証装置から、最新の履歴の認証子を読み出し前記履歴テーブルの最新の履歴の認証子との一致を検出することにより前記履歴が最新の履歴であることを検証する認証子検証手段と、を備えた履歴管理装置と、を具備することを特徴とする。

【0013】(5) 請求項5に対応する発明は、請求項1に対応する発明をコンピュータに実現させるプログラムを記録した記憶媒体である。

【0014】(6) 請求項6に対応する発明は、請求項9に対応する発明をコンピュータに実現させるプログラムを記録した記憶媒体である。

【0015】本願発明によれば、電子保管の個々の履歴の排他的論理和をとり、それにより得られる最新の認証子を例えばICカードのような耐タンパー性を有する装置に保管される。この最新の認証子は情報が不正に改ざんされることを防ぐため、装置の機能により正当なプロセスを経た場合にのみ、情報の更新が行われ、外部からの情報への直接のアクセスは一切不可である。これによりシステムの構成を簡単化することができる。この点につき、従来は電子データ保管システム全体を安全な装置に入れ、電子データ自体は例えばハードディスク装置に入れ装置外部に設けるが、履歴の管理装置はシステムの中に入っていて外部から不正にアクセスできないような構成になっている。このためシステム全体を収めるための耐タンパー性を有した箱を設ける必要がありコストがかさむという問題点を本願発明は解決することができる。

【0016】

【発明の実施の形態】以下、本発明の実施の形態につい

て図面を参照して説明する。

【0017】図1は本発明の実施の形態における電子データ保管システムの基本的な構成である。電子データ保管システム100はサーバ計算機1と履歴検証装置2とから構成される。サーバ計算機1は電子データ管理装置3と電子データ保存媒体4を有する。履歴検証装置2は電子データの原本性を保証する上で核となる装置であり、耐タンパー性を備えたハードウェアから構成される。具体的には、ICカード等が考えられる。電子データ管理装置3は特定の機能を備えたハードウェア、またはソフトウェアをインストールした計算機から構成される。電子データ管理装置3は電子データを保管・管理するためのインターフェース機能を有する。

【0018】図2は、本発明の電子データ保管システム100の概略図である。ユーザは電子データ保管システム100内の電子データ管理装置3に電子データ(電子文書等)を登録する。電子データ保管システム100は電子データの管理を行う電子データ管理装置3と、電子データが格納される、例えばハードディスク装置から構成される電子データ保存媒体4、及び例えばICカードにより実現される履歴検証装置2とから構成される。ここで、ユーザにより登録された電子データは電子署名等の認証情報がつけられて電子データ保存媒体4に格納される。このとき、電子データ管理装置3内にある履歴テーブルに、登録行為の情報が記載される。履歴テーブルはその真正性を保証するために認証子がつけられており、履歴が最新であることを保証するため、履歴の最新行の認証子(ここでは、認証子3)がシステムに装着された履歴検証装置(ICカード等に)2に安全に保管される。

【0019】図3は電子データ保存媒体4に格納される電子データD1の形態を示す。電子データ保存媒体4は電子データ管理装置3によって電子データD1の書き込み、読み出しが行われる。電子データ保存媒体4には電子データD1に添付情報D2が関連づけて格納される。添付情報D2は、電子データを一意に識別するためのID、作成者・日付等の属性情報、内容が改ざんされていないことを保証するためのメッセージ認証子が含まれる。IDは文書番号と改訂番号からなり、新規文書が保存されるたびに文書番号が更新されていく。改訂版の保存の場合には、文書番号は同一で改訂番号を更新する。

【0020】図4は電子データ管理装置3の構成を示す。電子データ管理装置3は履歴管理装置5、履歴検証装置アクセス装置6、メッセージダイジェスト作成装置7、メッセージ認証子検証装置8、電子データ管理装置制御装置9からなり、電子データ保存機能F1、電子データ検証機能F2を備え、これらの機能によりユーザは電子データの保管・管理を行う。メッセージダイジェスト作成装置7はメッセージダイジェスト作成機能F3を備え、電子データD1のメッセージ認証子作成に必要な

メッセージダイジェストを作成する。メッセージダイジェストは例えばハッシュ法を用いて作成される。メッセージ認証子検証装置8はメッセージ認証子検証機能F4を備え、電子データD1が改ざんされていないかを検証する。履歴検証装置アクセス装置6は履歴管理装置5からの処理要求を受け取り、履歴検証装置2へ送信する。履歴検証装置2の処理結果は履歴検証装置アクセス装置6を経て履歴管理装置5に返される。電子データ管理制御装置9はユーザからの要求入力を受け取り、各種の機能を実行する。

【0021】図5は履歴管理装置5の構成を示す。履歴管理装置5は履歴テーブル格納庫10と履歴管理制御装置11からなり、識別子発番機能F5、履歴検証機能F6、履歴登録機能F7をもつ。履歴テーブル格納庫10は電子データの保存の履歴を格納し、履歴管理制御装置11は電子データ管理制御装置9からの要求を受け、各種の機能を実行し、その結果を返す。

【0022】図6は履歴テーブル格納庫10に格納される履歴の形態を示す。履歴は履歴番号、識別子、属性情報、電子データのメッセージダイジェスト、認証子を列とする表形式からなる。

【0023】図7は履歴と認証子の関係を示している。認証子は履歴テーブルの内容が改ざんされていないことを検証するためにつけられる。最初の履歴について、履歴番号1番と電子データの識別子、属性情報、メッセージダイジェスト21から新たにメッセージダイジェスト23を作成する。作成されたメッセージダイジェスト23は暗号化され認証子1となる。図7でEは暗号化の処理を表す。なお、メッセージダイジェスト21は登録する電子データのメッセージダイジェストであって、登録する電子データが改ざんされているか否かを検証するためのものであり、メッセージダイジェスト23は履歴のメッセージダイジェストであり、履歴が改ざんされているか否かを検証するのに用いる。2番目以降の履歴に関しては、同様に作成されたメッセージダイジェストと直前の認証子との排他的論理和をとってから暗号化を行う。これにより履歴の一部が改ざんされる、あるいは履歴の順番が変更された場合には、認証子の整合性が取れなくなり、履歴が改ざんされたことが検知できる。さらに履歴の最新行の認証子を履歴検証装置2内に安全に保管することにより、履歴が最新の情報であることを保証する。

【0024】図8は履歴検証装置2の構成を示す。履歴検証装置2は電子データ用復号化鍵格納庫12、電子データ用暗号化鍵格納庫13、履歴用復号化鍵格納庫14、履歴用暗号化鍵格納庫15、最新認証子格納庫16、最新履歴番号格納庫17、履歴検証制御装置18からなり、認証子更新機能F8、認証子検証機能F9、履歴の認証子検証機能F10を備える。履歴検証装置2は電子データの原本性を保証する上で重要な情報を保持し

ており、情報が不正に改ざんされることを防ぐため、装置の機能により正当なプロセスを経た場合にのみ、情報の更新が行われ、外部からの情報への直接のアクセスは一切不可であるとする。また、電子データ用復号化鍵格納庫12、電子データ用暗号化鍵格納庫13、履歴用復号化鍵格納庫14、履歴用暗号化鍵格納庫15は一度情報を書き込んだ後は二度と書き込み、変更は不可である。履歴検証装置2の機能は認定を行う団体によって検査されたのち、各種の鍵が各鍵格納庫12乃至15に書き込まれる。さらに最新認証子格納庫16に初期コード（例えば0の羅列からなるコード）を、また最新履歴暗号格納庫17には0をそれぞれセットする。鍵、初期コード、初期値を書き込まれた履歴認証装置は認定団体によって認定・登録される。履歴検証制御装置18は履歴検証装置アクセス装置6を経由して機能実行要求を受け取り、処理結果を返す。

【0025】以下に各装置の機能を述べる。図9は電子データ管理装置3において、電子データ保存機能F1を実行したときのフローチャートを示す。電子データ保存機能F1では電子データD1、及び属性情報D4を入力として得る。改訂番の保存の場合には、さらに文書番号D5を入力として得る。始めにステップS1で、履歴管理装置5の後述する履歴検証機能F6を実行する。エラーが返された場合にはステップS9でエラーメッセージを出力し、終了する。すでに履歴の検証がなされ、履歴に改ざんのないことが確認されている場合には、このステップを外すことは可能である。ステップS1が正常に終了した場合には、ステップS3で履歴管理装置5の後述する識別子発番機能F5を実行し、新たな識別子D6を取得する。改訂番の場合には、文書番号D5を入力として識別子発番機能F5に渡す。エラーが返された場合には、ステップS9に進み、終了する。ステップS3が正常に終了した場合には、ステップS5でメッセージダイジェスト作成装置7のメッセージダイジェスト作成機能F3に電子データD1、属性情報D4、識別子D6を入力として与え、メッセージダイジェストD7を受け取る。次に、ステップS6で履歴管理装置5の後述する履歴登録機能F7に識別子D6、属性情報D4、メッセージダイジェストD7を入力として与える。エラーが返された場合は、ステップS9に進みエラーメッセージを出力して終了する。ステップS6が正常に終了した場合、メッセージ認証子D8を出力として得る。識別子D6と属性情報D4とメッセージ認証子D8をまとめて添付情報D2として、電子データD1と関連づけて電子データ保存媒体4に格納し、終了する。

【0026】図10は電子データ管理装置3において、電子データ検証機能F2を実行したときのフローチャートを示す。入力として検証する電子データD1の識別子D6を受け取る。始めにステップS10において、履歴管理装置5の履歴検証機能F6を実行する。ステップS

10が正常に終了した場合には、ステップS12において電子データ保存媒体4から識別子D6に対応する電子データD1とその添付情報D2を読み出し、ステップS13において電子データD1とその添付情報D2を入力としてメッセージ認証子検証装置8のメッセージ認証子検証機能F4を実行する。エラーが返された場合には、ステップS15に進み、終了する。ステップS13が正常に終了した場合には終了する。

【0027】メッセージ認証子検証機能F4はメッセージダイジェスト作成装置7のメッセージダイジェスト作成機能F3に電子データD1と添付情報D2から取り出した属性情報D4、識別子D6を入力として与え、メッセージダイジェストD7を受け取る。次に、履歴検証装置アクセス装置6を経由して履歴検証装置2の履歴の認証子検証機能F10にメッセージダイジェストD7及び添付情報D2から取り出したメッセージ認証子D8を入力として与え、実行する。履歴の認証子検証機能F10は電子データ用復号化鍵格納庫12に格納された鍵を用いて、メッセージ認証子を復号化し、得られたコードがメッセージダイジェストD7と等しいか検証する。等しくなければ履歴検証装置2はエラーメッセージを電子データ管理装置3に返す。メッセージ認証子検証装置8のメッセージ認証子検証機能F4は、履歴検証装置2の履歴の認証子検証機能F10がエラーを返した場合には、エラーを返し、それ以外は正常終了する。

【0028】図11は履歴管理装置5において、識別子発番機能F5を実行したときのフローチャートを示す。入力データとして、文書番号D5が与えられた場合には、改訂版の発番ということでステップS21に進む。文書番号D5が与えられない場合は、新規文書の発番ということでステップS17に進む。ステップS17では、履歴テーブル格納庫10を検索し、最新の文書番号を得る。これをbとすると、ステップS18においてbに1を加えて新たに文書番号を得る。これをb'とする。ステップS19で改訂番号をr=0とし、ステップS20で新たな識別子ID=(b', r) (識別子D6)を出力し、終了する。改訂版の発番の場合には、ステップS21においてb=文書番号D5とする。次にステップS22で履歴テーブル格納庫10を検索し、文書番号D5と等しい文書番号の識別子が存在するか確認する。存在しない場合には、不当な文書番号を入力されたということでステップS27に進み、エラーメッセージを出力して終了する。ステップS22が正常に終了した場合には、ステップS24に進み、履歴テーブル格納庫10を検索し、文書番号D5に対して最新の改訂番号(識別子内に含まれる)を得る。これをrとする。ステップS25においてrに1を加えてあらたに改訂番号を得る。これをr'とする。ステップS26で新たな識別子D6=(b, r')を出力し、終了する。

【0029】図12は履歴管理装置5において、履歴検

証機能F6を実行したときのフローチャートを示す。始めにステップS28で履歴テーブル格納庫10の履歴の行数を調べ、これをKで表す。又、変数としてkを用いし、k=1とする。次に、ステップS29において履歴テーブル格納庫10のk番目の行から、履歴番号D9、識別子D10、属性情報D11、メッセージダイジェストD12、認証子D13を読み出す。ステップS30においてk=1の場合にはステップS32に進む。それ以外の場合はステップS31において履歴テーブル格納庫10のk-1番目の行から認証子D14を読み出す。ステップS32において、履歴番号D9、識別子D10、属性情報D11、メッセージダイジェストD12、認証子D13、k=1でない場合にはさらに認証子D14を入力として履歴検証装置2の認証子検証機能F9を実行する。エラーが返された場合には履歴が改ざんされたものとしてステップS36に進み、エラーメッセージを出力して終了する。ステップS32が正常に終了した場合にはステップS34において、k=Kであるか調べる。k=Kであれば処理を終了する。k=KでなければステップS35においてkに1を加え、ステップS29に戻る。

【0030】図13は履歴管理装置5において、履歴登録機能F7を実行したときのフローチャートを示す。履歴登録機能F7では、識別子D6、属性情報D4、メッセージダイジェストD7を入力として受け取る。始めにステップS37で履歴テーブル格納庫10を検索し、識別子D6が重複しないことを確認する。重複している場合には不正な識別子としてステップS42に進み、エラーメッセージを出力して終了する。ステップS37が正常に終了した場合(識別子が重複していない場合)は、ステップS39に進み、識別子D6、属性情報D4、メッセージダイジェストD7を入力として履歴検証装置2の認証子更新機能F8を実行し、履歴番号D15、識別子D6、メッセージ認証子D8を出力として受け取る。ステップS41で履歴テーブル格納庫10に履歴番号D15、識別子D6、属性情報D4、メッセージダイジェストD7、認証子D16を新たな行に追加する。ステップS42でメッセージ認証子D8を出力し、終了する。

【0031】図14は履歴検証装置2において、認証子更新機能F8を実行したときのフローチャートを示す。認証子更新機能F8は識別子D6、属性情報D4、メッセージダイジェストD7を入力として得る。始めにステップS44で最新履歴番号格納庫17の履歴番号をKとする。Kに1を加え、K+1とする。これを新たな履歴番号D15とする。ステップS45で履歴番号D15、識別子D6、属性情報D4、メッセージダイジェストD7から新たにメッセージダイジェストD16を生成する。ステップS46において、履歴番号D15が1であるか否か調べ、1の場合はステップS48に進む。1でない場合はステップS47に進み、メッセージダイジェスト

D16と最新認証子格納庫16に格納されている最新の認証子D17との排他的論理和を取り、コードD18を得たのち、ステップS48に進む。ステップS48ではコードD18またはメッセージダイジェストD16を履歴用暗号化鍵格納庫15に格納されている暗号化鍵により暗号化し、新たな認証子D16を生成する。ステップS49では新たな認証子D16を最新認証子格納庫14に格納する。ステップS50で入力データのメッセージダイジェストD7を、電子データ用暗号化鍵格納庫13に格納されている暗号化鍵により暗号化しメッセージ認証子D8を生成する。ステップS51で履歴番号D15、認証子D16、メッセージ認証子D8を出力し、終了する。

【0032】図15は、履歴検証装置2において、認証子検証機能F9を実行した時のフローチャートを示す。認証子検証機能F9は入力として履歴番号D9、識別子D10、属性情報D11、メッセージダイジェストD12、認証子D13を、履歴番号D9が1でない場合にはさらに認証子D14を得る。ステップS52において、履歴番号D9、識別子D10、属性情報D11、メッセージダイジェストD12からメッセージダイジェストD19を作成する。ステップS53において、履歴番号D9が1の場合はステップS61において、メッセージダイジェストD19をコードD20として、ステップS55に進む。それ以外の場合は、ステップS54において、メッセージダイジェストD19と1つ前の認証子D14との排他的論理和をとり、コードD20を得たのち、ステップS55に進む。ステップS55で認証子D13を履歴用復号化鍵格納庫12の復号化鍵で復号化しコードD21を得る。ステップS56においてコードD20またはメッセージダイジェストD19とコードD21が等しいか否かを検証する。等しくなければ、履歴は改ざんされたものとしてステップS60へ進み、エラーメッセージを出力して終了する。等しければステップS57に進み、履歴番号D9が最新履歴番号格納庫15の履歴番号D15と等しいか否かを調べる。等しくなければ終了し、等しければ、ステップS58に進む。ステップS58では認証子D13が最新認証子格納庫14の最新の認証子D16と等しいか否かを検証する。等しければ終了し、等しくなければ履歴が最新のものでないということでステップS60へ進み、エラーメッセージを出力して終了する。

【0033】図16は履歴管理装置と履歴検証装置2との間のデータのやりとりを図式化したものである。なお、図15と同一部には同符号を付す。履歴管理装置5は履歴テーブル10内履歴番号、識別子、属性情報、メッセージダイジェスト、現在の認証子(D13)、1つ前の認証子(D14)を履歴検証装置2に送る。

【0034】履歴検証装置2はステップS52において、履歴管理装置5から送られた、履歴番号、識別子、

属性情報、メッセージダイジェストのメッセージダイジェストを作成する。次に、ステップS54において、作成したメッセージダイジェストと1つ前の認証子D14との排他的論理和をとる。そして、ステップS55において、認証子D13を復号化し排他的論理和により得られる値と比較する。ステップS56において、比較結果が不一致であれば、履歴検証装置2はその旨を示すエラーメッセージを履歴管理装置5に返す。一方、比較結果が一致する場合には、ステップS57において、履歴が最新の履歴か否かを判断する。最新の履歴でない場合には、履歴検証装置2は、履歴が改ざんされていない旨のメッセージを履歴管理装置5に送る。一方、最新の履歴の場合には、さらに認証子D13と最新認証子格納庫内の最新認証子が等しいか否かを判断する。等しくない場合には、その旨を示すエラーメッセージを履歴管理装置5に返し、等しい場合には、履歴の時系列の時系列の関係が改ざんされていない旨の通知を履歴管理装置5に返す。

【0035】なお、本発明は上記実施の形態に限定されない。例えば、電子データ用復号化鍵と履歴用復号化鍵、及び電子データ用暗号化鍵と履歴用暗号化鍵はそれぞれ同一でもよい。その場合には、履歴用復号化鍵格納庫14及び履歴用暗号化鍵格納庫15は省略してもよい。

【0036】また、暗号処理は共通鍵暗合方式でも公開鍵暗合方式でもよい。公開鍵暗号方式の場合には図17に示すように、履歴管理装置5の内部に電子データ復号化鍵格納庫12と履歴用復号化鍵格納庫14を備える。

【0037】電子データの検証を行うには、メッセージ認証子検証装置8のメッセージ認証子検証機能F4において、履歴管理装置5の電子データ用復号化鍵格納庫12に格納された鍵を用いて、メッセージ認証子を復号化し、得られたコードがメッセージダイジェストと等しいか検証する。

【0038】履歴の検証を行うには、履歴管理装置5で図12に示すフローチャートと図15に示すフローチャートの両方を実行する。このときのフローチャートは図18に示すようになる。図18では、ステップS58-Aにおいて、認証子が最新であることを検証するため、履歴検証装置2から最新認証子を読み出し履歴テーブル10の認証子と比較を行う。他は図12および図15と基本的に同じである。

【0039】図19は履歴管理装置5側において、履歴の検証を行う場合の履歴管理装置5と履歴検証装置2との間のデータのやりとりを図式化したものである。なお、図12および図15と同一部には同符号を付す。

【0040】履歴管理装置5はステップS28において、履歴テーブルのk番目の行を読む。次に、ステップS31において、k-1番目の行から認証子D14を読む。次に、ステップS52において、履歴番号、識別

子、属性情報、メッセージダイジェストのメッセージダイジェストを作成する。ステップS54において、作成したメッセージダイジェストと1つ前の認証子D14との排他的論理和を取る。ステップS55において、認証子D13を復号化し排他的論理和により得られる値と比較し、不一致であれば、エラーメッセージを出力する。一方、一致すれば、ステップS57において、履歴が最新の履歴か否かを判断する。最新の履歴でなければ、ステップS28に戻る。一方、最新の履歴であれば、履歴管理装置5は履歴検証装置2内の最新認証子格納庫16内の最新認証子を読み出し、認証子D13と等しいか否かを判断する(ステップS58(S59))。等しければ、その旨を示すフローチャートを出力し、等しければ履歴の時系列の関係が改ざんされていない旨の通知を出力する。

【0041】この場合には認証子の検証の大部分を履歴管理装置5で行うことで、履歴検証装置2の負担を減らすことができる。

【0042】また、電子データ管理システム100の運用方法によっては、履歴検証装置2の機能に対する団体の認定は省略できる。

【0043】

【発明の効果】この発明によれば、電子データを保管し管理する装置に、電子データ保存の履歴を記録する履歴テーブルと、履歴テーブルに対する改ざんの有無を検知するための認証情報を作成する手段と、履歴テーブルが最新であることを認証するための履歴検証手段と、認証情報を安全に管理する履歴検証装置を備える構成としたので、電子データの改ざん、消去を防止することができるとともに、電子データの原本性を確保することができる。

【図面の簡単な説明】

【図1】本発明の一実施の形態における電子データ保管システムの基本的な構成を示すブロック図である。

【図2】本発明一実施の形態における電子データ保管システムの概略図である。

【図3】上記実施の形態における電子データ保存媒体に格納される電子データD1の形態図である。

【図4】上記実施の形態における電子データ管理装置の構成を示すブロック図である。

【図5】上記実施の形態における履歴管理装置の構成を示すブロック図である。

【図6】上記実施の形態における履歴テーブル格納庫に格納される履歴の形態図である。

【図7】上記実施の形態における履歴と認証子の関係を示す図である。

【図8】上記実施の形態における履歴検証装置の構成を示すブロック図である。

【図9】上記実施の形態における電子データ管理装置において、電子データ保存機能F1の処理を示すフローチャートである。

【図10】上記実施の形態における電子データ管理装置において、電子データ検証機能F2の処理を示すフローチャートである。

【図11】上記実施の形態における履歴管理装置において、識別子発番機能F5の処理を示すフローチャートである。

【図12】上記実施の形態における履歴管理装置において、履歴検証機能F6の処理を示すフローチャートである。

【図13】上記実施の形態における履歴管理装置において、履歴登録機能F7の処理を示すフローチャートである。

【図14】上記実施の形態における履歴検証装置において、認証子更新機能F8の処理を示すフローチャートである。

【図15】上記実施の形態における履歴検証装置において、認証子検証機能F9の処理を示すフローチャートである。

【図16】上記実施の形態において、履歴管理装置5と履歴検証装置2との間のデータのやりとりを示すフローチャートである。

【図17】本発明の第2の実施の形態における電子データ保管システムのブロック図である。

【図18】図12において、認証子の検証機能を履歴検証装置の外部で行うときの処理を示すフローチャートである。

【図19】上記第2の実施の形態において、履歴管理装置5と履歴検証装置2との間でデータのやりとりを示すフローチャートである。

【図20】電子証明書の構造を示す説明図である。

【図21】サーバー認証の仕組みを示す説明図である。

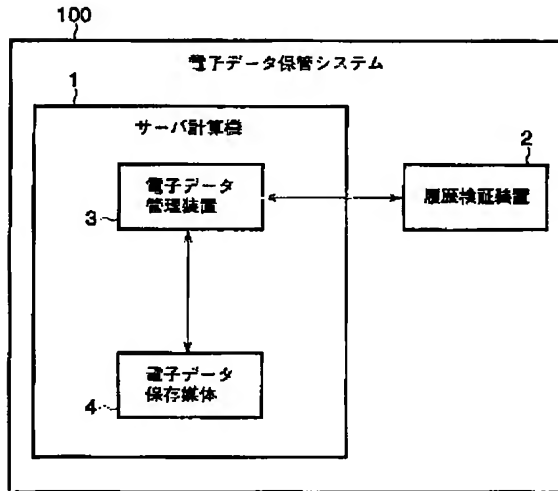
【符号の説明】

- 1…サーバ計算機
- 2…履歴検証装置
- 3…電子データ管理装置
- 4…電子データ保存媒体
- 5…履歴管理装置
- 6…履歴検証装置アクセス装置
- 7…メッセージダイジェスト作成装置
- 8…メッセージ認証子検証装置
- 9…電子データ管理制御装置
- 10…履歴テーブル格納庫
- 11…履歴管理制御装置
- 12…電子データ用復号化鍵格納庫
- 13…電子データ用暗号化鍵格納庫
- 14…履歴用復号化鍵格納庫
- 15…履歴用暗号化鍵格納庫
- 16…最新認証子格納庫
- 17…最新履歴番号格納庫

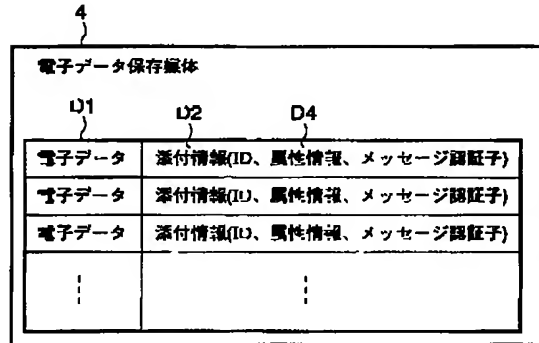
18...履歴検証制御装置

100...電子データ保管システム

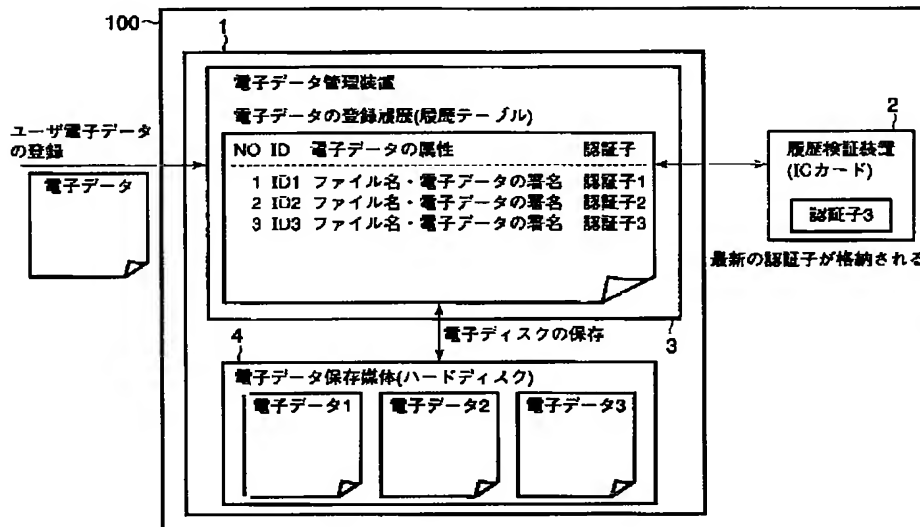
【図1】



【図3】



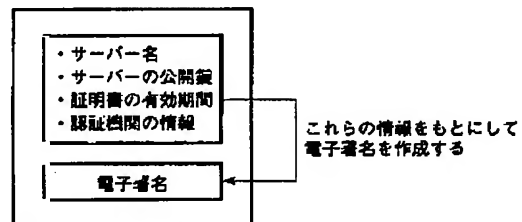
【図2】



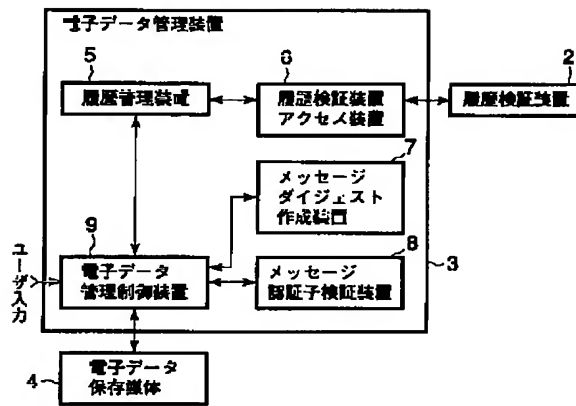
【図7】

23
認証子1=E((1', ID1, 属性情報1, メッセージダイジェスト1)の
メッセージダイジェスト)
21
認証子2=E((2', ID2, 属性情報2, メッセージダイジェスト2)の
メッセージダイジェストと認証子1との排他的論理和)
認証子3=E((3', ID3, 属性情報3, メッセージダイジェスト3)の
メッセージダイジェストと認証子2との排他的論理和)
認証子4=E((4', ID4, 属性情報4, メッセージダイジェスト4)の
メッセージダイジェストと認証子3との排他的論理和)
.....

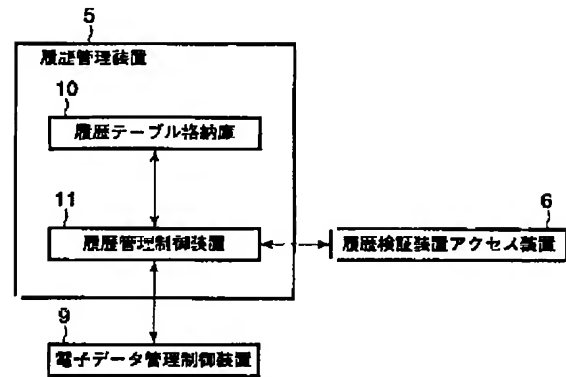
【図20】



【図4】



【図5】

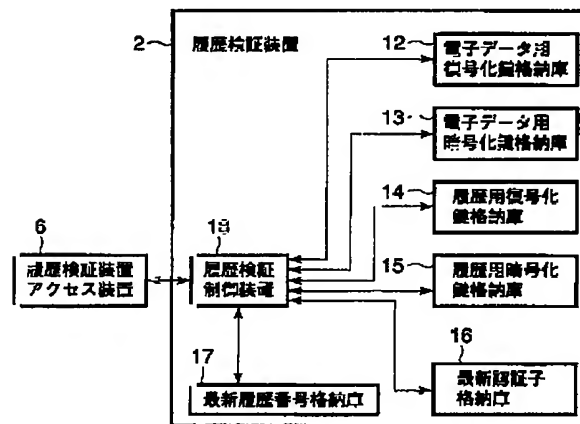


【図6】

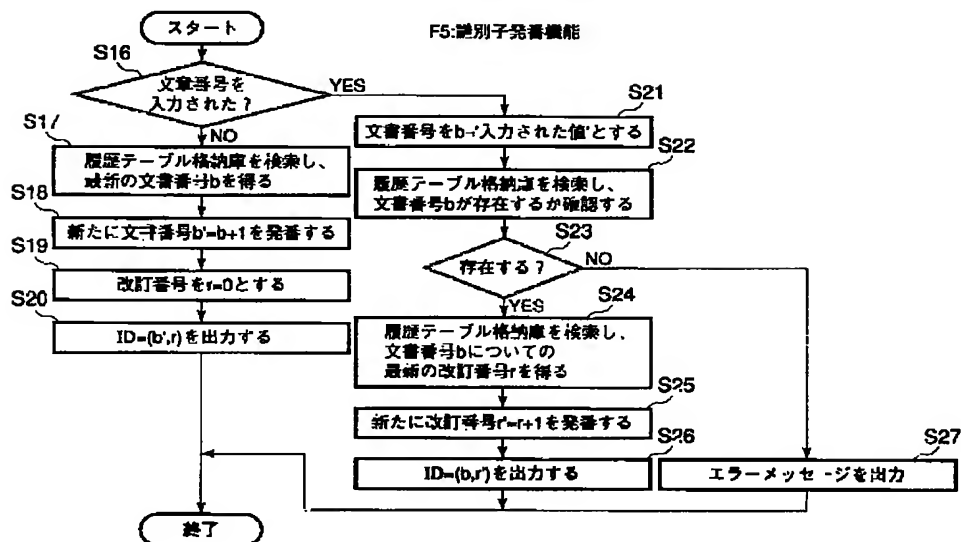
10
履歴テーブル格納庫

1	ID1	属性情報1	MD1	認証子1
2	ID2	属性情報2	MD2	認証子2
3	ID3	属性情報3	MD3	認証子3
⋮	⋮	⋮	⋮	⋮

【図8】

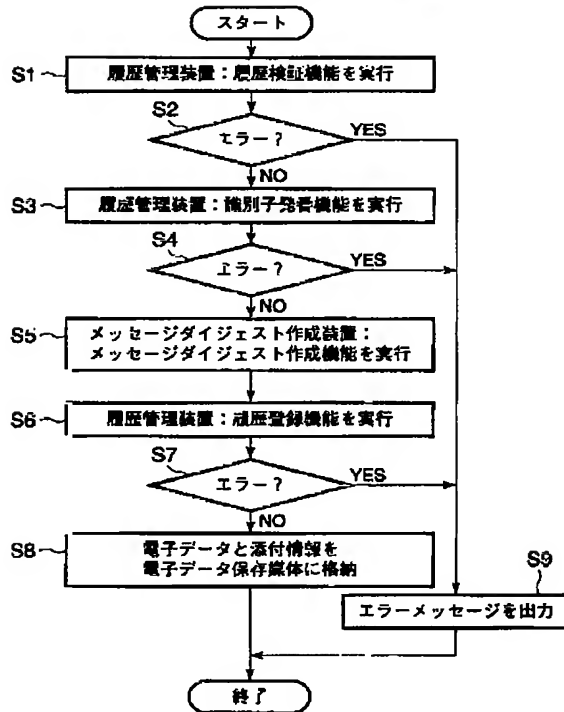


【図11】



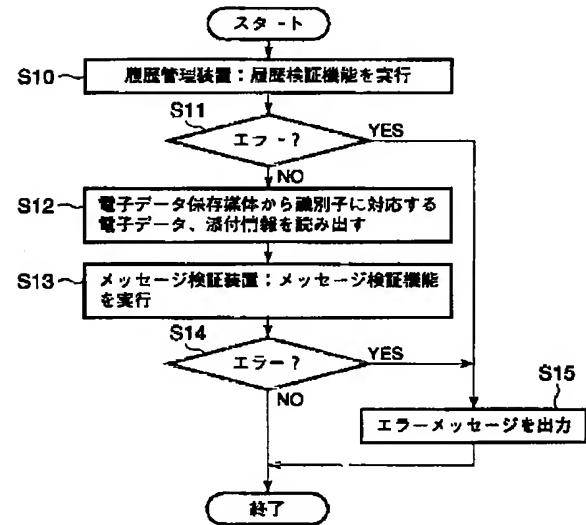
【図9】

F1:電子データ保存機能



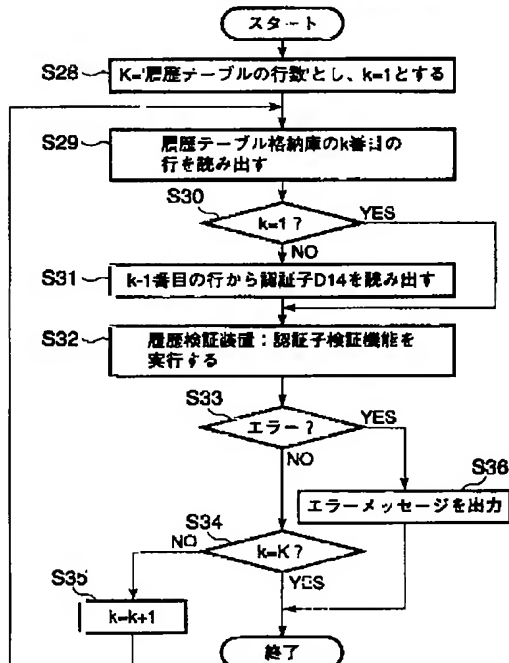
【図10】

F2:電子データ検証機能



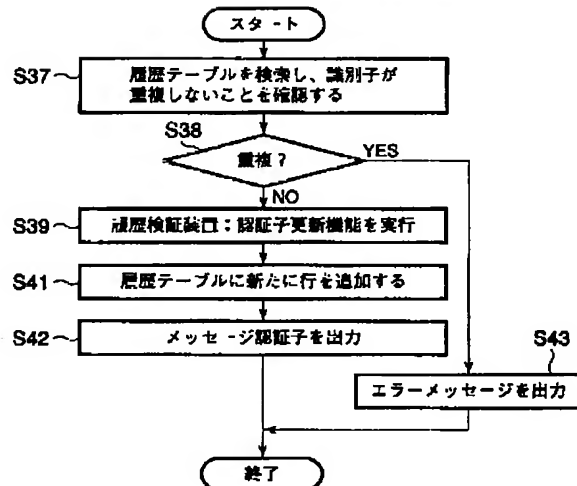
【図12】

F6:履歴検証機能

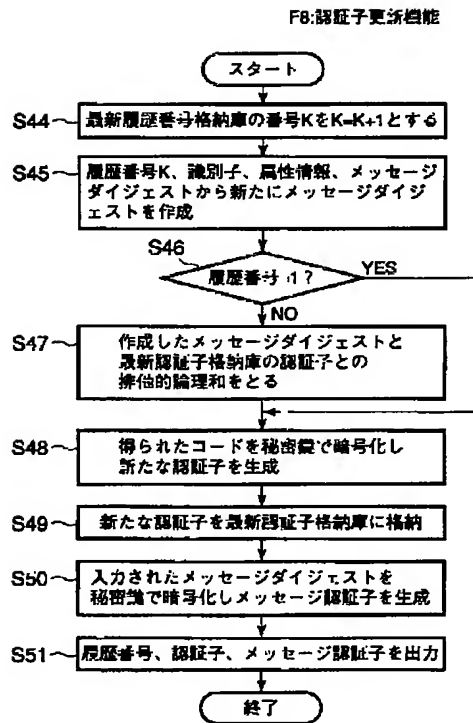


【図13】

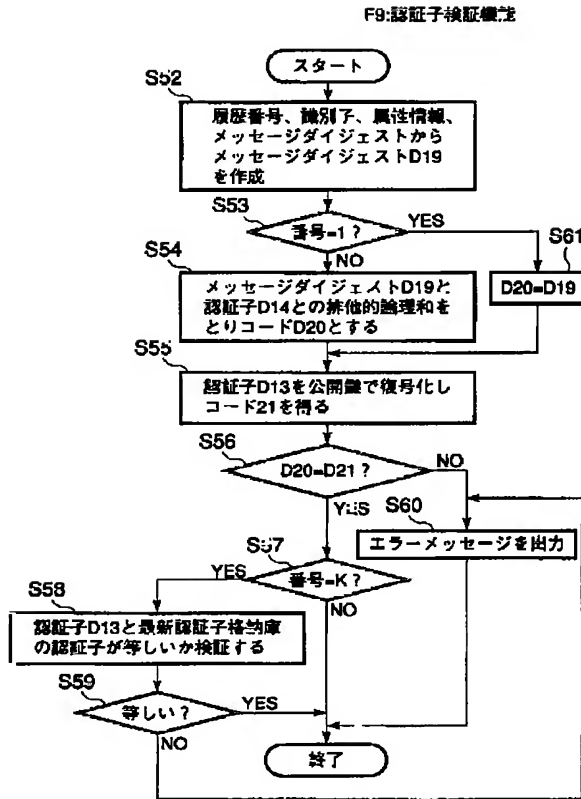
F7:履歴登録機能



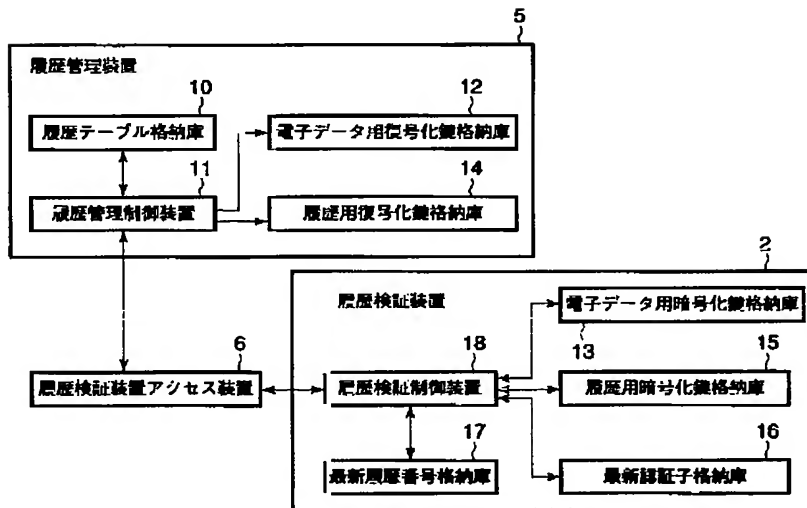
【図14】



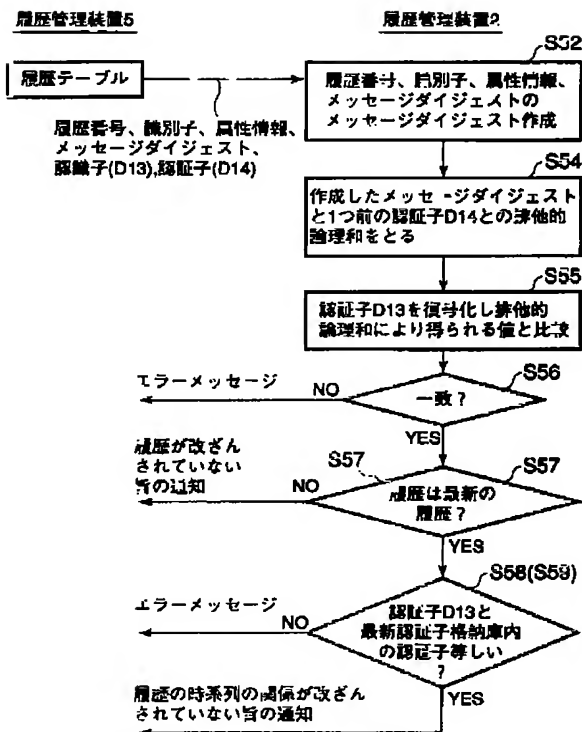
【図15】



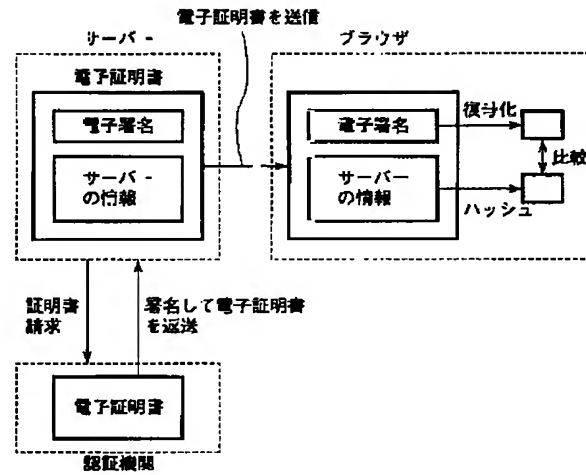
【図17】



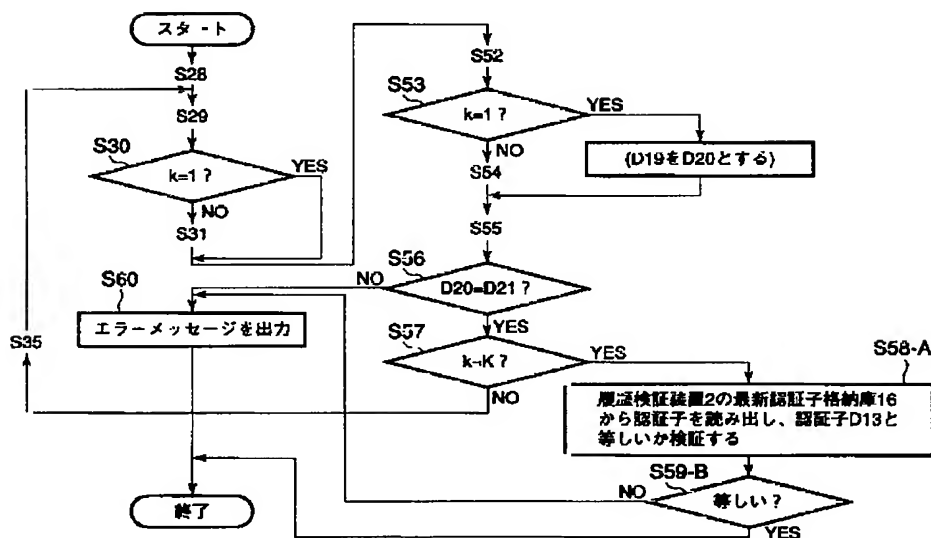
【図16】



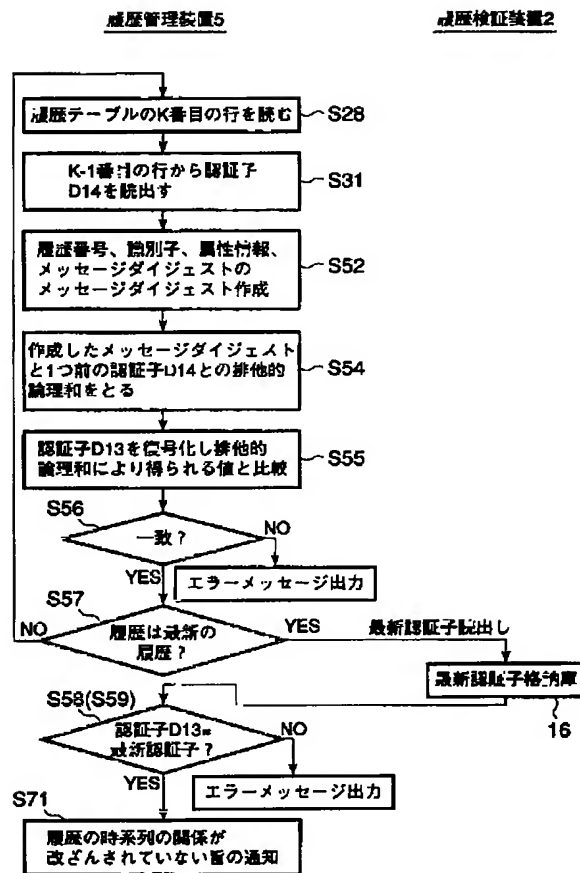
【図21】



【図18】



【図19】



フロントページの続き

(51) Int. Cl.⁷
G 0 6 K 19/10

識別記号

F I
G 0 6 K 19/00(参考)
R